TI - Session key generation system for common key encryption system edits hash processed data into predetermined bit length and outputs session key data

PR - JP20010088800 20010326

PN - JP2002290391 A 20021004 DW200307 H04L9/08 009pp

PA - (TOCM) TOYO COMMUNICATION EQUIP CO

IC - H04L9/08

AB - JP2002290391 NOVELTY - A multiplexer (8) multiplexes common key data and session identification information. A hash processing unit (17) performs hash processing to multiplexed data, based on predetermined hash function processing algorithm. A data edit unit (18) edits hash processed data into predetermined bit length and outputs session key data.

- DETAILED DESCRIPTION - An INDEPENDENT CLAIM is included for encryption device.
- USE - For common key encryption system used for internet communication.
- ADVANTAGE - Enables reliable encryption of data and reduces communication cost.
- DESCRIPTION OF DRAWING(S) - The figure shows the block diagram of the encryption device and decoder in the common key encryption system. (Drawing includes non-English language text).
- Multiplexer 8
- Hash processing unit 17
- Data edit unit 18
- (Dwg.1/4)

OPD - 2001-03-26

AN - 2003-071002 [07]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2002－290391
（P2002－290391A）
(43)公開日　平成14年10月４日(2002.10.4)

(51)Int.Cl.'	識別記号	ＦＩ	テーマコード'(参考)
Ｈ０４Ｌ　9/08		Ｈ０４Ｌ　9/00	６０１Ｃ　５Ｊ１０４
			６０１Ｅ

審査請求　未請求　請求項の数５　ＯＬ　（全９頁）

(21)出願番号　特願2001－88800(P2001－88800)

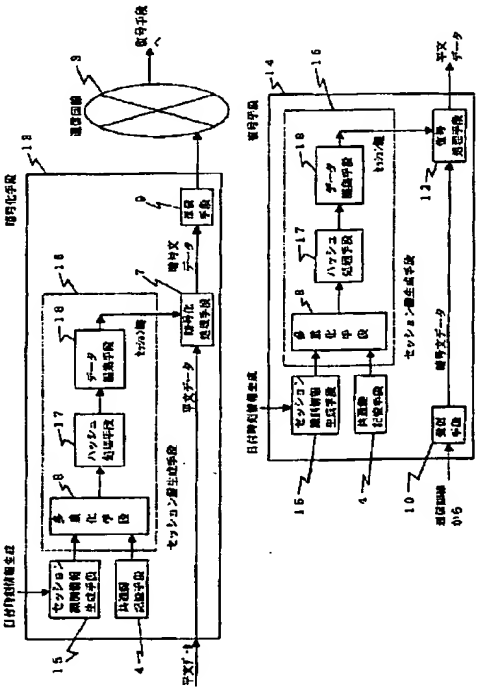
(22)出願日　平成13年３月26日(2001.3.26)

(71)出願人　000003104
東洋通信機株式会社
神奈川県川崎市幸区塚越三丁目484番地
(72)発明者　市瀬　浩
神奈川県高座郡寒川町小谷二丁目１番１号
東洋通信機株式会社内

Ｆターム(参考)　5J104 AA01 AA16 AA36 EA06 EA18
JA01 NA02 NA03 NA12 NA22

(54)【発明の名称】　共通鍵暗号方式におけるセッション鍵生成方式及び暗号化／復号装置。

(57)【要約】　（修正有）
【課題】本発明は、共通鍵から生成したセッション鍵によって平文データ或いは暗号文データを暗号化或いは復号する暗号化／復号装置において、通信コストを抑えられる暗号強度の強い共通鍵暗号方式におけるセッション鍵生成方式と暗号化／復号装置を提供することを目的とする。
【解決手段】共通鍵データとセッション識別情報からセッション鍵データを生成するセッション鍵生成方式において、共通鍵データ及びセッション識別情報を多重化処理し多重化データを出力する多重化手段８と、所定のハッシュ関数処理アルゴリズムに基づき多重化手段の供給する多重化データを処理しハッシュ処理データを出力するハッシュ処理手段１７と、ハッシュ処理手段が出力するハッシュ処理データを所定ビット長に編集しセッション鍵データを出力するデータ編集手段１８とを備えたことを特徴とするセッション鍵生成方式。



【特許請求の範囲】
【請求項１】共通鍵データとセッション識別情報からセッション鍵データを生成するセッション鍵生成方式において、
前記共通鍵データ及び前記セッション識別情報を多重化処理し多重化データを出力する多重化手段と、所定のハッシュ関数処理アルゴリズムに基づき前記多重化手段の供給する多重化データを処理しハッシュ処理データを出力するハッシュ処理手段と、前記ハッシュ処理手段が出力するハッシュ処理データを所定ビット長に編集しセッション鍵データを出力するデータ編集手段とを備えたことを特徴とするセッション鍵生成方式。
【請求項２】共通鍵データとセッション識別情報からセッション鍵データを生成するセッション鍵生成方式において、
前記共通鍵データ及び前記セッション識別情報を多重化処理し多重化データを出力する多重化手段と、所定ビット長のカウントデータを保持出力するカウンタと、前記多重化手段が出力する多重化データと前記カウンタが出力するカウントデータとを保持するレジスタと、所定のハッシュ関数処理アルゴリズムに基づき前記レジスタが保持する該多重化データとカウントデータとを処理しハッシュ処理データを出力するハッシュ処理手段と、前記ハッシュ処理手段が出力するハッシュ処理データを所定ビット長に編集しセッション鍵候補データを出力するデータ編集手段と、前記データ編集手段から供給されるセッション鍵候補データと特定のデータパターンとを比較照合し該セッション鍵候補データが特定のデータパターンに該当しないときは該セッション鍵候補データをセッション鍵データとして出力する判定手段とを備えたセッション鍵生成方式であって、前記判定手段において比較照合する該セッション鍵候補データが特定のデータパターンに該当したときは前記カウンタが保持出力するカウントデータを更新するように制御したことを特徴とするセッション鍵生成方式。
【請求項３】前記共通鍵データ及び前記カウンタが保持するカウントデータを前記判定手段に供給すると共に、該カウンタにおいてカウントデータの更新を所定回数実行したとき判定手段に供給されるセッション鍵候補データがいずれも前記特定のデータパターンに該当したときは、前記判定手段に供給された共通鍵データをセッション鍵データとして出力するように制御したことを特徴とする請求項２記載のセッション鍵生成方式。
【請求項４】共通鍵から生成したセッション鍵によって平文データを暗号化する暗号化装置において、
前記請求項１、請求項２或いは請求項３記載のセッション鍵生成方式のいずれかと、前記セッション鍵生成方式にて生成したセッション鍵データに基づき平文データを所定のアルゴリズムにて処理し暗号文データを出力する暗号化処理手段と、前記暗号化処理手段が出力する暗号文データを通信回線に出力する送信手段とを備えたことを特徴とする暗号化装置。
【請求項５】前記請求項４記載の暗号化装置によって生成された暗号文データを復号する復号装置であって、
前記請求項１、請求項２或いは請求項３記載のセッション鍵生成方式のいずれかと、前記請求項４記載の暗号化装置が出力する暗号文データを通信回線を介して受信処理する受信手段と、前記セッション鍵生成方式にて生成したセッション鍵データに基づき前記受信手段が出力した暗号文データを所定のアルゴリズムににて復号処理し平文データを出力する復号処理手段とを備えたことを特徴とする復号装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、共通鍵暗号方式におけるセッション鍵生成の暗号技術に関する。
【０００２】
【従来の技術】近年、インターネット等の情報インフラがグローバルな規模で整備され本格的な高度情報化社会を迎えるに至った。暗号技術は高度情報化社会を支える重要な基盤技術であり、様々な暗号技術が研究開発されている。なかでも、共通鍵暗号方式は暗号化すべき情報を高速に処理できるという利点を有しており、その応用分野は広い。共通鍵暗号方式は、情報の送り手側が情報を共通鍵で暗号化したものを通信手段を使って搬送し、情報の受け手側ではこれを送り手側と全く同じ共通鍵で復号する方式である。
【０００３】現代の暗号技術においては、情報の送り手が毎回同じ共通鍵を使い続けたとしても暗号化した情報から共通鍵を推測することはほとんど不可能である。しかしながら、搬送すべき情報に定常性があるとその性質に着目して暗号化した情報を解読できる可能性が高まることも事実である。このため、情報を搬送する毎に異なる鍵を使用し暗号強度を高める工夫を凝らしているが、一般的には固定的な共通鍵を基にセッション鍵を疑似乱数的に生成できるようにしておき、このセッション鍵で情報を暗号化するようにしている。このようにすると、情報の搬送の回数等によって、定期的或いは不定期に暗号化する鍵（セッション鍵）が変更されるので暗号強度を高めることができる。
【０００４】図４は従来の共通鍵暗号方式における暗号化／復号装置のブロック図を示したものである。図４において、送信側は平文データを暗号化し暗号文データを出力する暗号化手段１を備え、受信側は前記暗号化手段１が出力した暗号文データを復号する復号手段２を備えており、前記暗号化手段１（送側）と復号手段２（受側）との間は通信回線３で接続されている。
【０００５】また、暗号化手段１は、所定の共通鍵データを記憶する共通鍵記憶手段４と、疑似乱数的にセッション識別情報を発生するセッション識別情報生成手段５

と、前記共通鍵記憶手段４の出力する共通鍵データを前記セッション識別情報にて暗号化しセッション鍵データを出力するセッション鍵生成手段６と、平文データを前記セッション鍵データにて暗号化し暗号文データを出力する暗号化処理手段７と、前記暗号化処理手段７からの暗号文データ及び前記セッション識別情報生成手段５からのセッション識別情報を多重化処理し送信データとして出力する多重化手段８と、前記送信データを通信回線３へ送信する送信手段９とを備えている。

【０００６】更に、復号手段２は、前記送信データを通信回線３を介して受信し受信データとして供給する受信手段１０と、前記受信手段１０が供給する受信データから暗号文データとセッション識別情報とをそれぞれ分離出力する多重分離手段１１と、共通鍵データを記憶する共通鍵記憶手段４と、前記共通鍵記憶手段４からの共通鍵データを前記多重分離手段１１からのセッション識別情報で暗号化しセッション鍵データを生成出力するセッション鍵生成手段６と、多重分離手段１１から供給された暗号文データを前記セッション鍵データで復号し平文データを出力する復号処理手段１２とを備えている。

【０００７】なお、この例では一方を送信側とし他方側を受信側としているが、それぞれに復号手段２及び暗号化手段１を設け、双方向で暗号文データをやりとりすることも可能であるが、ここでは説明を簡単化するため図示を省略する。

【０００８】図４に示した従来の共通鍵暗号方式における暗号化／復号装置は以下のように動作する。最初に送信側で平文データを暗号化する過程について説明する。まず、セッション識別情報生成手段５は疑似乱数的にセッション識別情報を生成しこれをセッション鍵生成手段６及び多重化手段８へ供給するようになっている。ここで、前記セッション識別情報は送信手段９が暗号文データを送出する回数や日付等に応じて定期的或いは不定期に更新されるようになっている。

【０００９】そこで、セッション鍵生成手段６は共通鍵記憶手段４から供給される共通鍵データを前記セッション識別情報で暗号化しセッション鍵データを生成出力する。更に暗号化処理手段７は入力された平文データを前記セッション鍵データによって暗号化し暗号文データを多重化手段８へ供給する。多重化手段８は前記セッション識別情報生成手段５から供給されたセッション識別情報と前記暗号文データとを多重化し送信データとして送信手段９へ供給する。送信手段９は通信回線３にアクセスし前記送信データを送出する。

【００１０】次に、復号手段２で前記送信データを復号する過程について説明する。まず、受信手段１０が通信回線３を介して前記送信データを受信し、これを受信データとして多重分離手段１１へ供給する。多重分離手段１１は前記受信データから暗号文データとセッション識別情報とをそれぞれ分離しセッション鍵生成手段６及び復号処理手段１２に供給する。一方、セッション鍵生成手段６には共通鍵記憶手段４から共通鍵データが供給されている。セッション鍵生成手段６はこれを前記セッション識別情報にて暗号化しセッション鍵データを復号処理手段１２に供給する。復号処理手段１２は前記セッション鍵データを用いて多重分離手段１１から供給された暗号文データを復号し平文データとして出力する。

【００１１】ここで、復号手段２において共通鍵記憶手段４に記憶した共通鍵データは、暗号化手段１において共通鍵記憶手段４に記憶した共通鍵データと同じものであり、更にそれぞれが備えるセッション鍵生成手段６は同じ暗号処理アルゴリズムを有している。従って、復号手段２において生成されるセッション鍵データは暗号化手段１で生成されたものと全く等しいものとなるので、復号処理手段１２は暗号文データを復号することが可能となっている。

【００１２】このように、従来の共通鍵暗号方式における暗号化／復号装置においては、送信側（暗号化手段１）で平文データを暗号化する際、セッション鍵を生成するためのセッション識別情報を暗号文データに付加して送信し、受信側（復号手段２）では送られてきた送信データからセッション識別情報を分離しこれを用いてセッション鍵を生成したので、暗号文データを復号することが可能となっていた。

【００１３】

【発明が解決しようとする課題】しかしながら、従来の共通鍵暗号方式における暗号化／復号装置には以下のような問題点があった。すなわち、送信側（暗号化手段１）から受信側（復号手段２）に対して本来の暗号文データにセッション鍵識別情報を付加して伝送し、受信側はこれを分離して復号のためのセッション鍵データを生成していた。

【００１４】従って、本来の暗号文データにセッション識別情報を付加していたので、送信手段９で伝送すべきデータ量が増加してしまい、その分通信コストが増加し通信時間も長くなってしまうという問題があった。更に、暗号化手段１において生成した暗号文データを送信履歴として保存し蓄積しておくような場合や、或いは復号手段２において受信した暗号文データを受信履歴として保存し蓄積していくような場合も、保存すべきファイルのデータ量が増大してしまうので大容量の記憶媒体を必要とする問題もあった。

【００１５】本発明は、上記問題点を解決するためになされたものであって、送信側から受信側へセッション識別情報を伝達することなくセッションを確立させることのできる、共通鍵暗号方式におけるセッション鍵生成方式と暗号化／復号装置を提供することを目的とする。

【００１６】上記問題点を解決するために、本発明に係わる共通鍵暗号方式におけるセッション鍵生成方式と暗号化／復号装置の請求項１記載の発明は、共通鍵データ

とセッション識別情報からセッション鍵データを生成するセッション鍵生成方式において、前記共通鍵データ及び前記セッション識別情報を多重化処理し多重化データを出力する多重化手段と、所定のハッシュ関数処理アルゴリズムに基づき前記多重化手段の供給する多重化データを処理しハッシュ処理データを出力するハッシュ処理手段と、前記ハッシュ処理手段が出力するハッシュ処理データを所定ビット長に編集しセッション鍵データを出力するデータ編集手段とを備えたものである。

【００１７】本発明に係わる共通鍵暗号方式におけるセッション鍵生成方式と暗号化／復号装置の請求項２記載の発明は、共通鍵データとセッション識別情報からセッション鍵データを生成するセッション鍵生成方式において、前記共通鍵データ及び前記セッション識別情報を多重化処理し多重化データを出力する多重化手段と、所定ビット長のカウントデータを保持出力するカウンタと、前記多重化手段が出力する多重化データと前記カウンタが出力するカウントデータとを保持するレジスタと、所定のハッシュ関数処理アルゴリズムに基づき前記レジスタが保持する該多重化データとカウントデータとを処理しハッシュ処理データを出力するハッシュ処理手段と、前記ハッシュ処理手段が出力するハッシュ処理データを所定ビット長に編集しセッション鍵候補データを出力するデータ編集手段と、前記データ編集手段から供給されるセッション鍵候補データと特定のデータパターンとを比較照合し該セッション鍵候補データが特定のデータパターンに該当しないときは該セッション鍵候補データをセッション鍵データとして出力する判定手段とを備えたセッション鍵生成方式であって、前記判定手段において比較照合する該セッション鍵候補データが特定のデータパターンに該当したときは前記カウンタが保持出力するカウントデータを更新するように制御したものである。

【００１８】本発明に係わる共通鍵暗号方式におけるセッション鍵生成方式と暗号化／復号装置の請求項３記載の発明は、前記請求項２記載のセッション鍵生成方式において、前記共通鍵データ及び前記カウンタが保持するカウントデータを前記判定手段に供給すると共に、該カウンタにおいてカウントデータの更新を所定回数実行したとき判定手段に供給されるセッション鍵候補データがいずれも前記特定のデータパターンに該当したときは、前記判定手段に供給された共通鍵データをセッション鍵データとして出力するように制御したものである。

【００１９】本発明に係わる共通鍵暗号方式におけるセッション鍵生成方式と暗号化／復号装置の請求項４記載の発明は、共通鍵から生成したセッション鍵によって平文データを暗号化する暗号化装置において、前記請求項１、請求項２或いは請求項３記載のセッション鍵生成方式のいずれかと、前記セッション鍵生成方式にて生成したセッション鍵データに基づき平文データを所定のアルゴリズムにて処理し暗号文データを出力する暗号化処理手段と、前記暗号化処理手段が出力する暗号文データを通信回線に出力する送信手段とを備えたものである。

【００２０】本発明に係わる共通鍵暗号方式におけるセッション鍵生成方式と暗号化／復号装置の請求項５記載の発明は、前記請求項４記載の暗号化装置によって生成された暗号文データを復号する復号装置であって、前記請求項１、請求項２或いは請求項３記載のセッション鍵生成方式のいずれかと、前記請求項４記載の暗号化装置が出力する暗号文データを通信回線を介して受信処理する受信手段と、前記セッション鍵生成方式にて生成したセッション鍵データに基づき前記受信手段が出力した暗号文データを所定のアルゴリズムににて復号処理し平文データを出力する復号処理手段とを備えたものである。

【００２１】

【発明の実施の形態】以下図示した実施の形態例に基づいて本発明を詳細に説明する。図１は本発明に係わる、共通鍵暗号方式における暗号化／復号装置の実施の形態例を示したブロック図である。図１において、送信側は平文データを暗号化し暗号文データを出力する暗号化手段１３を備え、受信側は前記暗号化手段１３が出力した暗号文データを復号する復号手段１４を備えており、前記暗号化手段１３（送側）と復号手段１４（受側）との間は所定の通信回線３で接続されている。

【００２２】また、暗号化手段１３は、共通鍵データを記憶する共通鍵記憶手段４と、入力された日付時刻情報に基づきセッション識別情報を生成出力するセッション識別情報生成手段１５と、前記共通鍵データ及び前記セッション識別情報からセッション鍵データを生成出力するセッション鍵生成手段１６と、前記セッション鍵データにて平文データを暗号化し暗号文データを出力する暗号化処理手段７と、前記暗号化処理手段７からの暗号文データを通信回線３へ送信する送信手段９とを備えている。

【００２３】そして、前記セッション鍵生成手段１６は、前記共通鍵記憶手段４の出力する共通鍵データ及び前記セッション識別情報生成手段１５の出力するセッション識別情報を多重化し多重化データを出力する多重化手段８と、前記多重化データを所定のハッシュ関数アルゴリズムにて処理し所定ビット長のハッシュ処理データを出力するハッシュ処理手段１７と、前記ハッシュ処理手段１７からのハッシュ処理データを所定ビット長に編集しセッション鍵データを前記暗号化処理手段７に供給するデータ編集手段１８とを備えている。

【００２４】更に、復号手段１４は、前記暗号化手段１３から送信された暗号文データを通信回線３を介して受信し受信データとして出力する受信手段１０と、共通鍵データを記憶する記憶手段４と、入力された日付時刻情報に基づきセッション識別情報を生成出力するセッション識別情報生成手段１５と、前記共通鍵データ及び前記セッション識別情報からッション鍵データを生成するセ

ッション鍵生成手段１６と、前記セッション鍵データにて前記受信データ（暗号文データ）を復号し平文データを出力する復号処理手段１２とを備えている。

【００２５】なお、復号手段１４が備えるセッション鍵生成手段１６については、暗号化手段１３の構成において説明したものと同一なので説明を省略する。また、送信側及び受信側にもそれぞれ復号手段１４及び暗号化手段１３を設け、双方向で暗号文データをやりとりすることが可能であるが説明を簡単化するため図示を省略する。

【００２６】以下、図１に示した本発明に係わる、共通鍵暗号方式における暗号化／復号装置の実施の形態例についてその動作を説明する。最初に、送信側で平文データを暗号化する過程について説明する。まず、セッション識別情報生成手段１５は日付時刻情報を入手し、セッション識別情報を生成する。例えば、現在の日付が２００１年3月１５日ならば、２００１０３１５と数値化した日付を、各桁毎１バイト（＝８ビット）の文字コードに変換し、全体で８ビット×８＝６４ビットのセッション識別情報とする。

【００２７】ここで、前記日付時刻情報は暗号化手段１３がリアルタイムクロック等の時刻手段を備えるようにしてここから供給するようにしてもよいし、或いは別途パソコン等のオペレーションシステムから日付情報を供給してもらうか、または高精度の日付時刻情報を持った時刻手段（例えば、ＧＰＳ受信機の時刻情報等）から供給してもらってもかまわない。

【００２８】そこで、セッション識別情報生成手段１５は生成した６４ビットのセッション識別情報を多重化手段８に供給する。一方、共通鍵記憶手段４には所定ビット長の共通鍵データが記憶保存されており、これが前記多重化手段８に供給されている。多重化手段８は前記共通鍵データ及びセッション識別情報を多重化し、多重化データを生成出力する。ここで、前記多重化データは共通鍵データの先頭或いは後方にセッション識別データを付加したものであってもよいし、一定の規則に基づき共通鍵データ列の中にセッション鍵データを挿入するようにしてもよい。

【００２９】そして、ハッシュ処理手段１７は多重化手段８から供給された多重化データを所定のハッシュ関数アルゴリズムを用いて処理し所定ビット長のハッシュ処理データを出力する。ここで、ハッシュ関数処理とは入力された所定ビット長のデータを圧縮して小さいデータ列を生成するプログラムであって、現在電子署名におけるメッセージダイジェスト（要約文）の生成に良く使われている。また、ハッシュ関数プログラムの代表的なものとしてＭＤ４、ＭＤ５、ＳＨＡ或いはＳＨＡ－１といったものが主に利用されているが詳細は省略する。

【００３０】次に、データ編集手段１８は前記ハッシュ処理手段１７から供給されたハッシュ処理データの中から所定ビット分を選択するか、或いはビット長を増やして編集し所定ビット長のセッション鍵データを生成出力する。なお、生成したセッション鍵データは共通鍵データと同じビット長としているが、セッション鍵データのビット長を共通鍵データのビット長より長くしても構わないが、ほとんど暗号強度は変わらない。逆に短くすると暗号強度が落ちてしまうので、セッション鍵データは共通鍵データのビット長と同じとするのが好ましい。

【００３１】そこで、暗号化処理手段７は前記データ編集手段１８から供給されたセッション鍵データに基づき入力された平文データを暗号化し暗号文データとして出力する。送信手段９は前記暗号文データを送信データとして通信回線３に送出する。ここまで送信側において平文データを暗号化する過程について説明した。

【００３２】次に、前記送信データを受信側で復号する過程について説明する。まず、セッション識別情報鍵生成手段１５にてセッション鍵データを生成し出力する。ここで、セッション識別情報生成手段１５において生成されるセッション識別情報及び共通鍵記憶手段４に記憶された共通鍵データは暗号化手段１３において生成されたものと全く同じものであり、且つハッシュ処理手段１７及びデータ編集手段１８についても暗号化手段１３のものと全く同じ処理を実行しているのでデータ編集手段１８から出力されるセッション鍵データは暗号化手段１３において生成したものと全く同じものとなる。

【００３３】従って、受信手段１０が通信手段３から供給された送信データを受信データとして復号処理手段１２に供給し、復号処理手段１２は前記データ編集手段１８から供給されたセッション鍵データを基にして前記受信データを復号するので、暗号文データを元の平文データに復号することが可能となる。

【００３４】なお、暗号化手段１３及び復号手段１４において、セッション識別情報生成手段１５が生成するセッション識別情報は日付時刻情報を基に生成したものであると説明した。従って、日付が変わるとセッション識別情報は前日のものとは全く異なる情報となり、生成されるセッション鍵データも日毎に変更されるので、暗号強度に優れた通信を行うことが可能となる。また、送信側において本来の暗号文データにセッション識別情報を付加する必要がなくなるので、送信データのデータ量を削減でき、通信回線３の利用時間も短縮でき通信コストを節約できる利点がある。更に暗号化手段１３と復号手段１４の構成がほぼ同じものとなるので、システム全体の構築が簡単になり、システムのコストを低減することができる。

【００３５】また、本説明においては、送信側で暗号化したものが、受信側で瞬時に処理されるリアルタイム処理を前提として説明しているが、送信側（暗号化側）及び受信側（復号側）の処理に時刻差がかなり生じるような場合であってもよい。例えば、一方から電子メールを

暗号化して他方に送信し、他方側は受信した電子メールを数日後に開封するといった場合、セッション識別情報の更新周期を一日一回から１週間に一回に変更するといったことも可能である。いずれにせよ、暗号化する対象（アプリケーション）に合わせて更新周期を適切に設定すればよい。

【００３６】以上説明した、本発明に係わる共通鍵暗号方式における暗号化／復号装置において、セッション鍵生成手段１６で生成するセッション鍵データは、ハッシュ処理手段１７にて生成したハッシュ処理データをデータ編集手段１８にて所定ビット長に編集してセッション鍵データとして使用したが、この実施例においては生成されたセッション鍵データが、００・・・・００や１１・・・・１１等の特定パターンとなってしまう可能性がある。このような場合暗号文データが解読されやすくなるという欠点を有するので、これを解決するためセッション鍵生成方式の第２の実施例を提案する。

【００３７】図２はセッション鍵データ生成手段１６の第２の実施例を示したブロック図である。図２に示したセッション鍵データ生成手段１６の第２の実施例は、共通鍵記憶手段４及びセッション識別情報生成手段１５からそれぞれ供給された共通鍵データ及びセッション識別情報を多重化し多重化データを出力する多重化手段８と、所定ビット長のカウントデータを保持出力するカウンタ１９と、前記多重化情報及び前記カウントデータを保持するレジスタ２０と、前記レジスタ２０が保持するレジスタデータを所定のハッシュ関数アルゴリズムにて処理し所定ビット長のハッシュ処理データを出力するハッシュ処理手段１７と、前記ハッシュ処理手段１９からのハッシュ処理データを所定ビット長に編集しセッション鍵候補データを出力するデータ編集手段１８と、前記データ編集手段１８から供給されたセッション鍵候補データを特定のデータパターンと比較照合し該当しない場合はセッション鍵データとして出力する判定手段２１と、前記カウンタ１９のカウントデータの初期値を設定する初期値設定手段２２とを備えている。

【００３８】図２に示したセッション鍵生成手段は以下のように動作する。まず、セッション識別情報生成手段１５は日付時刻情報を入手し、セッション識別情報を生成する。例えば、現在の日付が２００１年３月１５日ならば、２００１０３１５と数値化した日付を、各桁毎１バイト（＝８ビット）の文字コードに変換し、全体で８ビット×８＝６４ビットのセッション識別情報とする。ここで、前記日付時刻情報は図１の暗号化手段１３がリアルタイムクロック等の時刻手段を備えるようにしてここから供給するようにしてもよいし、或いは別途パソコン等のオペレーションシステムから日付情報を供給してもらうか、または高精度の日付時刻情報を持った時刻手段（例えば、ＧＰＳ受信機の時刻情報）から供給してもらってもかまわない。

【００３９】そこで、セッション識別情報生成手段１５は生成した６４ビットのセッション識別情報を多重化手段８に供給する。一方、共通鍵記憶手段４には所定ビット長の共通鍵データが記憶保存されており、これが前記多重化手段８に供給されている。多重化手段８は前記共通鍵データ及びセッション識別情報を多重化し、多重化データを生成出力する。ここで、前記多重化データは共通鍵データの先頭或いは後方にセッション識別データを付加したものであってもよいし、一定の規則に基づき共通鍵データ列の中にセッション鍵データを挿入するようにしてもよい。

【００４０】一方、初期値設定手段２２を用いてカウンタ１９のカウントデータの初期値を設定する。ここでは、カウンタ１９を８ビットカウンタとして、初期値を００００００００と設定したものとする。レジスタ２０は前記カウンタ１９の初期値をその下位ビットに格納するとともに、多重化手段８から供給された多重化データをその上位ビットに格納する。そして格納したカウンタ１９の初期値及び多重化データをレジスタデータとしてハッシュ処理手段１７に出力する。

【００４１】そして、ハッシュ処理手段１７はレジスタ２０から供給されたレジスタデータを所定のハッシュ関数アルゴリズムを用いて処理し所定ビット長のハッシュ処理データを出力する。次に、データ編集手段１８は前記ハッシュ処理手段１９から供給されたハッシュ処理データの中から所定ビット分を選択するか、或いはビット長を増やして編集し所定ビット長のセッション鍵候補データを生成出力する。なお、生成したセッション鍵候補データは共通鍵データと同じビット長としているが、セッション鍵候補データのビット長を共通鍵データのビット長より長くしても構わないがほとんど暗号強度は変わらない。逆に短くすると暗号強度が落ちてしまうので、セッション鍵候補データは共通鍵データのビット長と同じとするのが好ましい。

【００４２】次に、判定手段２１は前記データ編集手段１８から供給されたセッション鍵候補データを予め登録された特定パターンデータ（ここでは、判定手段２１に００・・・・００や１１・・・・１１等の特定パターンが複数登録されているものとする）と比較照合し、該当しない場合はこれをセッション鍵データとして出力する。

【００４３】一方、前記セッション鍵候補データが特定パターンに該当した場合は、判定手段２１はカウンタ制御信号をカウンタ１９に送出する。カウンタ１９は前記カウンタ制御信号に従い、カウントデータを初期値からカウントアップ（ここでは００００００００１となる）させる。レジスタ２０は前記００００００００１となったカウントデータを下位ビットに読み込み、上位ビットに格納した多重化データと共にハッシュ処理手段１７へ出力する。ハッシュ処理手段１７はこれを処理し所定ビット

長のハッシュ処理データを出力しデータ編集手段１８に供給する。

【００４４】データ編集手段１８は前記ハッシュ処理データを編集し共通鍵候補データとして判定手段２１に出力する。判定手段２１は再びセッション鍵候補データを特定パターンと比較照合し、該当しない場合はこれをセッション鍵データとして出力する。該当しない場合は再びカウンタ制御信号をカウンタ１９に供給し、以上の手順を繰り返す。

【００４５】このように、編集手段１８で生成したセッション鍵候補データを判定手段２１にて特定パターンと比較照合するので、セッション鍵候補データが特定パターンとなってもセッション鍵データとして出力せず、別途特定パターンに該当しないようにセッション鍵候補データを生成しなおして出力することが可能となる。

【００４６】なお、カウンタ１９が８ビットカウンタの場合、カウントデータとしては２５６通りの組み合わせができるが、カウンタ１９のビット数が少ない場合には生成されたセッション鍵候補データがいずれも特定パターンに該当してしまうといった可能性も考えられる。これを回避するためセッション鍵生成手段１６の第３の実施例を提案する。

【００４７】図３にセッション鍵生成手段の第３の実施例のブロック図を示す。図３に示したセッション鍵生成手段の第３の実施例は、図２のセッション鍵生成手段に信号線が２本追加されている。すなわち、共通鍵記憶手段４に記憶した共通鍵データ、及びカウンタ１９のカウンタデータを直接判定手段２１に供給するようにしたものである。

【００４８】そして、データ編集手段１８にて生成したセッション鍵候補データがいずれも特定パターンに該当してしまう様な場合、即ち、カウンタ１９からのカウントデータが一巡したのにもかかわらずセッション鍵データが決定しないとき、判定手段２１は供給された共通鍵データをそのままセッション鍵データとして出力するようにする。このようにすれば、確実に最適なセッション鍵データを出力することができるし、カウンタ１９のビット数を小さくすることも可能となる。勿論カウンタ１９のビット数を８ビットにしたものにこれを適用してもよい。

【００４９】

【発明の効果】本発明は以上説明したように、共通鍵から生成したセッション鍵によって平文データ或いは暗号文データを暗号化或いは復号する暗号化／復号装置において、暗号化側と復号側にそれぞれ独立に共通のセッション鍵生成手段を備え、暗号化側で生成したセッション鍵データと同じものを復号側で生成できるように構成したので、従来暗号化側において本来の暗号文データにセッション鍵データを生成するためのセッション識別情報を付加し、暗号化側で送信される送信データのデータ量が増大し、通信コストが増えてしまった問題を解決し、通信コストを抑えられる暗号強度の強い共通鍵暗号方式におけるセッション鍵生成方式と暗号化／復号装置を提供する上で著効を奏す。

【００５０】

【図面の簡単な説明】

【図１】本発明に係わる共通鍵暗号方式における暗号化／復号装置の実施の形態例を示したブロック図。

【図２】従来の共通鍵暗号方式における暗号化／復号装置の実施の形態例を示したブロック図。

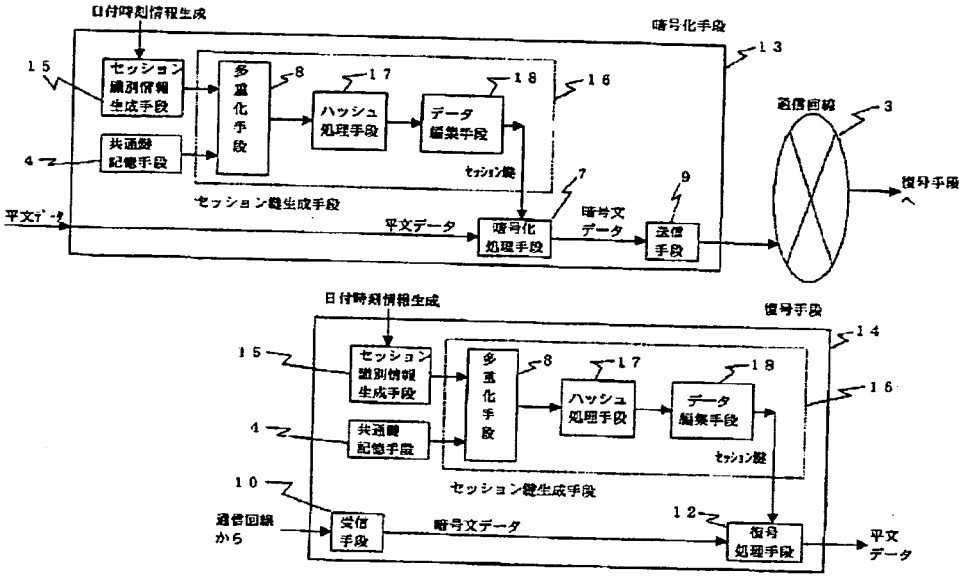
【図３】セッション鍵生成方式の第２の実施例を示したブロック図。

【図４】セッション鍵生成方式の第３の実施例を示したブロック図。

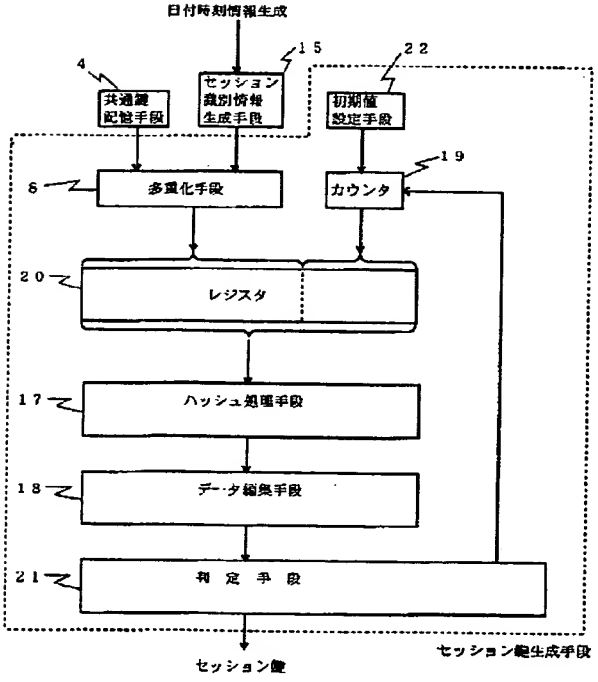
【符号の説明】

１、１３･･･暗号化手段
２、１４･･･復号手段
３･･･通信手段
４･･･共通鍵記憶手段
５、１５･･･セッション識別情報生成手段
６、１６･･･セッション鍵生成手段
７･･･暗号化処理手段
８･･･多重化手段
９･･･送信手段
１０･･･受信手段
１１･･･多重分離手段
１２･･･復号処理手段
１７･･･ハッシュ処理手段
１８･･･データ編集手段
１９･･･カウンタ
２０･･･レジスタ
２１･･･判定手段
２２･･･初期値設定手段

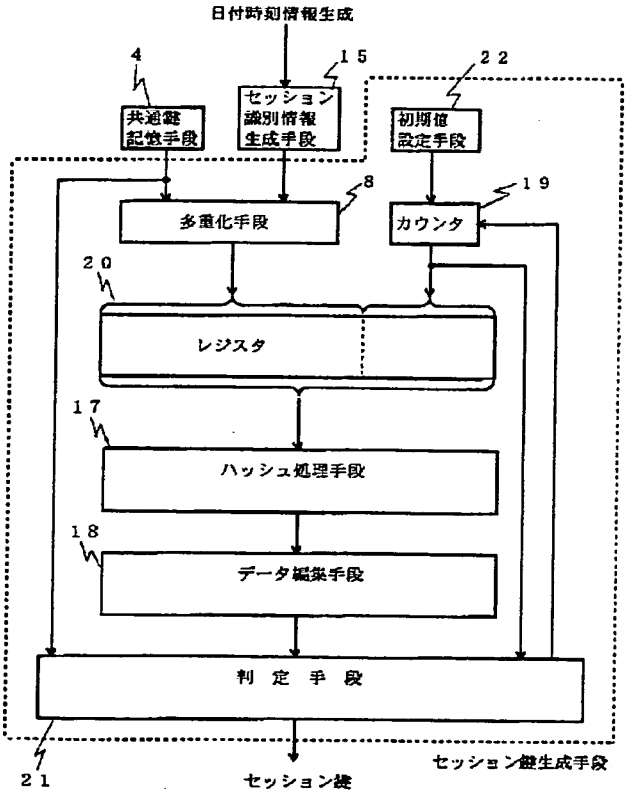
【図1】


日付時刻情報生成
暗号化手段
13
15
セッション識別情報生成手段
多重化手段
8
17
ハッシュ処理手段
18
データ編集手段
16
4
共通鍵記憶手段
セッション鍵
セッション鍵生成手段
通信回線
3
復号手段へ
7
9
平文データ
平文データ
暗号化処理手段
暗号文データ
送信手段
日付時刻情報生成
復号手段
14
15
セッション識別情報生成手段
多重化手段
8
17
ハッシュ処理手段
18
データ編集手段
16
4
共通鍵記憶手段
セッション鍵
セッション鍵生成手段
10
通信回線から
受信手段
暗号文データ
12
復号処理手段
平文データ

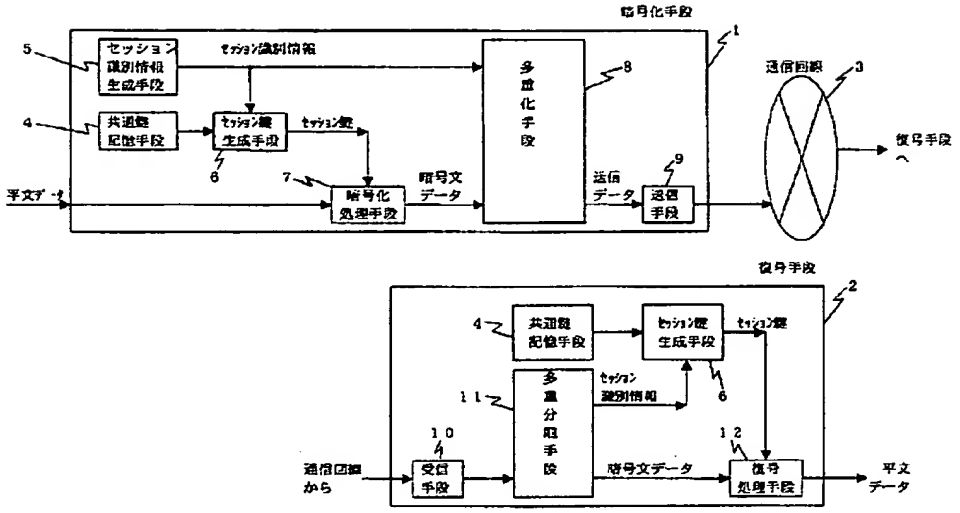
【図2】


日付時刻情報生成
4
15
22
共通鍵記憶手段
セッション識別情報生成手段
初期値設定手段
6
多重化手段
カウンタ
19
20
レジスタ
17
ハッシュ処理手段
18
データ編集手段
21
判定手段
セッション鍵
セッション鍵生成手段

【図3】


日付時刻情報生成
4
15
22
共通鍵記憶手段
セッション識別情報生成手段
初期値設定手段
多重化手段
8
カウンタ
19
20
レジスタ
17
ハッシュ処理手段
18
データ編集手段
判定手段
21
セッション鍵
セッション鍵生成手段

【図4】


暗号化手段
1
5
セッション識別情報生成手段
ｾｯｼｮﾝ識別情報
4
共通鍵記憶手段
ｾｯｼｮﾝ鍵生成手段
ｾｯｼｮﾝ鍵
6
7
暗号化処理手段
暗号文データ
多重化手段
8
送信データ
9
送信手段
通信回線
3
復号手段へ
平文ﾃﾞｰﾀ
復号手段
2
4
共通鍵記憶手段
ｾｯｼｮﾝ鍵生成手段
ｾｯｼｮﾝ鍵
11
多重分離手段
ｾｯｼｮﾝ識別情報
6
10
受信手段
12
復号処理手段
暗号文データ
通信回線から
平文データ